DEPARTMENT OF THE NAVY
CHIEF OF NAVAL EDUCATION AND TRAINING
250 DALLAS ST
PENSACOLA FLORIDA 32508-5220

CNETINST 3300.1
OS45
23 JAN 2001

CNET INSTRUCTION 3300.1

Subj: ANTITERRORISM/FORCE PROTECTION (AT/FP) PLAN

Ref: (a) DoD Directive 0-2000.12
(b) DoD Directive 0-2000.12-H
(c) SECNAVINST 3300.2
(d) OPNAVINST 3300.53
(e) OPNAVINST 5530.14C
(f) OPNAVINST 3120.32C
(g) OPNAVINST 5530.13B
(h) OPNAVINST 5580.1
(i) CNETINST 5530.2G
(j) SECNAVINST 3300.3
(k) OPNAVINST 3591.1C
(l) SECNAVINST 5530.4B

Encl: (1) Antiterrorism/Force Protection Policy Guide for CNET Activities

1. Purpose. To implement enclosure (1), promote a common understanding, and strengthen FP support among Chief of Naval Education and Training (CNET) commands through guidance in references (a) through (l).

2. Issue. References (a) through (l) shall be used throughout CNET to establish and issue uniform and minimum physical security standards that reduce the risk to assets (personnel, equipment, and facilities) from acts of terrorism and political turbulence. Each command shall evaluate assigned functions from a FP perspective to: (1) identify those of potential interest to adversaries under various circumstances; (2) isolate relative physical security requirements; and, (3) identify individual and organizational responsibilities to ensure an acceptable physical security posture.

3. Applicability. This instruction applies to all Department of Defense (DoD) personnel, their families, facilities, and material resources for reducing vulnerability to terrorism within CNET commands.

4. Background/Discussion. References (a) through (l) provide security policy and guidance for all activities. By combining physical security measures, personnel security awareness, intelligence information, and command attention, most risks can be overcome.

5. Policy

a. A FP Plan that clearly establishes operational responsibilities is required by all CNET commands. The Plan requires coordination at all levels and will include the host command. As a minimum, the plan must include: (1) collection, analysis, and distribution of terrorist threat information; (2) procedures for response to terrorist actions; and, (3) enhanced AT procedures to protect command interests (e.g., off-installation housing, personnel, families of personnel, high risk personnel, equipment, weapons, facilities, etc.). The plan must also address the use, by terrorists, of weapons of mass destruction (WMD), vulnerabilities to assets if such use occurs, and planned countermeasures. The plan should include procedures for the immediate notification to higher authority, when information is first received of such a potential use in that command's area of responsibility.

b. Under the FP concept, an acceptable level of security can be achieved when special emphasis is placed upon: (1) security awareness; (2) training for all personnel, including family members; (3) risk assessments/analysis; (4) development of a comprehensive physical security plan; (5) annual physical security surveys to evaluate command security posture; and, (6) integrating terrorist threat conditions (THREATCONs) into contingency plans.

c. The ultimate responsibility for physical security within CNET lies with the individual unit commander. This responsibility is clearly defined in references (e) and (f).

d. To mitigate the effectiveness of a vehicle bomb attack, commanders shall be continually vigilant against allowing vehicle parking near high-density, soft-target buildings. Every attempt should be made to establish a minimum of a 30-foot standoff distance, where possible. During THREATCON Bravo, commanders will achieve an 80-foot or more vehicle standoff distance from high-density soft targets. At THREATCON Charlie or Delta, a minimum of a 100-foot standoff distance should be achieved. Centralized or remote parking should be instituted at THREATCON Charlie or higher. Additionally, traffic patterns shall be a consideration in AT/FP plans.

e. Regional and Installation Commanders will program for their respective installations a set of recognizable building alarms (different from fire alarms) for use in potential bomb emergencies. Frequent drills are required to familiarize personnel with bomb alarm procedures, individual responsibilities, and designated safe-haven points. This type of preparedness training is meant to take advantage of the critical few minutes between alert and terrorist attack on buildings.

(1) New DoD AT/FP construction standards incorporate FP alarm systems as a new DoD requirement.

(2) Billeting and primary gathering structures require an internal and external emergency audible alarm system that is unique from fire or other alarm systems. This system should be able to be activated from within the building and a remote 24-hour monitored site. A bomb alarm system will be incorporated into plans for new construction.

f. AT/FP Level I training will be conducted in accordance with enclosure (1), and a report containing the number of personnel trained by month, total for quarter, and total for calendar year will be forwarded to CNET (OS45) no later than the 10th day of January, April, July, and October for the preceding quarter.

g. AT/FP plans will be exercised at least annually, and a copy of the after-action report forwarded to CNET (OS45) within 30 days of the exercise. Simulation should be kept to a minimum and only used to simulate things that would create a major disruption in the command's ability to meet their mission.

h. Navy Blue Dart messages. Commanders will ensure training is conducted on required response to Navy Blue Dart messages.

6. Action. CNET Commanders shall implement the provisions of enclosure (1).

7. Reports. Report control symbols CNET 3300-1 and 3300-2 have been assigned to the reporting requirements contained in paragraphs 5f and 5g and are approved for 3 years from the date of this instruction.

D. L. BREWER, III
Vice CNET

CNETINST 3300.1
23 JAN 2001

Distribution (CNETINST 5218.2D):
Lists I through V

Stocked:
CHIEF OF NAVAL EDUCATION AND TRAINING
CODE 0041
CNET
PENSACOLA FL 32508-5220

ANTITERRORISM/FORCE PROTECTION POLICY GUIDE FOR CNET ACTIVITIES

AT/FP POLICY GUIDE FOR CNET ACTIVITIES

1. Applicability

a. This guide sets forth the minimum physical security/ force protection (PS/FP) requirements for all CNET activities and is applicable to all DoD personnel, their families, facilities, and material resources.

b. Regional and Installation Commanders will publish implementing instructions to subordinate and tenant commands. Installation PS/FP plans will be reviewed at least annually by the Regional/Installation Commander to ensure completeness of plans and compliance with this and other applicable instructions.

2. Oversight Assessments and Assist Visits

a. Regional and Installation Commanders' Oversight Assessment. Regional and Installation Commanders will, at least triennially, conduct an oversight assessment to determine subordinate and tenant command adherence to implementing instructions. Records of this assessment will be maintained for at least 3 years. Specific areas to be addressed in the oversight assessment are:

(1) Qualification/designation of security officer

(2) Security education

(a) AT/FP training program

(b) Documentation of AT/FP training

(3) Security planning

(a) Risk analysis and risk management

(b) Physical security surveys/plans

(c) Interservice Support Agreements (ISSAs)/ Memorandums of Understanding (MOUs)/Memorandums of Agreement (MOAs)

(d) Standard Operating Procedures (SOPs)

(e) PS/FP review and assessment process

(f) Arms, ammunition, and explosives (AA&E) handling procedures and program

(4) Compensatory measures for waivers and exceptions; contingency plans for waived/excepted areas

(5) Loss prevention

(a) Education

(b) Administrative inspection of vehicles

(c) Access control measures and procedures

b. Assist Visits. Regional and Installation Commanders should schedule assist visits with the Naval Criminal Investigative Service (NAVCRIMINVSERV) Law Enforcement/Physical Security (LEPS) teams to review security procedures. LEPS provides technical expertise in the evaluation of a command's overall security program.

c. Integrated Vulnerability Assessments (IVA). Regions and installations with 300 personnel or more will be scheduled once every 3 years for an IVA, conducted either by the Joint Staff/ Defense Threat Reduction Agency or Chief of Naval Operations (CNO), to assess installation security programs and posture, per reference (a). For installations with fewer than 300 personnel, the CNET Security Program Manager, with assistance from CNO, will conduct a VA every 3 years using CNO's vulnerability assessment checklist.

d. PS assist visits/assessments will include appropriate plan of action and milestones (POA&M) to ensure discrepancies are corrected or planned action taken.

3. Security Planning

a. Readiness Standards. CNET readiness standards or security posture is based upon readiness criteria established by the Integrated Warfare Architecture (IWAR). CNET minimum acceptable readiness standard for PS/FP is C-3. Commands are required to notify the CNET Physical Security Program Manager if their security posture falls below the minimum acceptable readiness standard. Security requirements for CNET aviation assets may vary due to mission, location and vulnerability, operational readiness and value, classification, and replacement costs.

(1) **C1** - Layered security, 24-hour manned gates or open base posture if base policy dictates. Able to counter all Threat Types (Low through Maximum). Waterfront security maintained at Level One; Aviation assets security at Level Two. Armed security forces man posts 24 hours. Short response time (less than 5 minutes) with containment capability. Frequent random administrative vehicle inspections. Military Working Dogs (MWDs) supporting missions and fleet contingencies 80-100 percent. For manpower: 95-100 percent of the manpower requirements determined by the Shore Manpower Requirements Determination (SMRD) Program is funded.

(2) **C2** - Enclaved security, 12-hour manned gates or open base posture if base policy dictates. Able to counter Threat Types Low, Intermediate, and Advanced but not Maximum. Waterfront security not manned at Level One. Armed Security forces man posts 12 hours. Slow response time (5-15 minutes) with limited containment capability. MWDs supporting missions and fleet contingencies 60-79 percent. For manpower: 90-94 percent of the manpower requirements determined by the SMRD Program are funded.

(3) **C3** - Open base posture, 24-hour unmanned gates, if 24-hour manned gates is the base policy. Only able to counter Threat Types Low and limited Intermediate. Waterfront and Aviation assets vulnerable. Unarmed watchstanders man egress/ ingress. Lengthy response time (16-45 minutes) with poor containment capability. Few random administrative vehicle inspections. MWDs supporting missions and fleet contingencies 40-59 percent. For manpower: 85-89 percent of the manpower authorizations determined by the SMRD Program are funded.

(4) **C4** - Cannot meet mission requirements. For manpower: 0-84 percent of the manpower authorizations determined by the SMRD Program are funded.

b. PS/FP Plans

(1) As a general guidance tool/template, the Joint Staff J34, Combating Terrorism Organization publishes an AT/FP Planning Template that may be used to develop Regional and Installation PS/FP plans. This template is available electronically by using the following URL: http://nmcc20a.nmcc.smil.mil/~dj3cleap/j34pubsdocs/j34pubdoc.html or by contacting CNET (OS45).

(2) The coordination of installation and tenant command PS/FP planning is paramount to ensure maximum FP effectiveness.

All CNET commands will develop and publish a comprehensive PS/FP plan. The PS plan and AT/FP plan are one and the same provided that they cover crisis management standard operating procedures (i.e., Incident Response Plan, THREATCON implementation plan to include a barrier plan (barrier deployment locations, barrier storage locations and barrier transportation), personnel alerting system, and command center establishment procedures and security). Minimally, the PS/FP plan requires coordination at all levels to work in concert with the command disaster preparedness and recovery, mass casualty and WMD plans. Regional and Installation Commanders will ensure procedures are in place to:

(a) Implement a command and control structure and priorities of action in response to terrorist actions occurring on their installation or those areas under their jurisdiction.

(b) Collect, analyze and distribute terrorist threat information in coordination with local Naval Criminal Investigative Service (NCIS) representatives to ensure broad dissemination both up and down the chain of command.

(c) Implement proactive random antiterrorism measures (RAMs) and direct reactive terrorist-incident and recovery responses from attacks against mission essential assets and command interest areas for each THREATCON (e.g., aviation assets, communications systems, waterfronts, bulk petroleum storage areas, equipment, weapons systems and storage facilities, government family housing, high personnel concentration locations, family members, high-risk personnel, etc.).

(d) Request Fleet Antiterrorist Security Team (FAST) augmentation for contingency operations.

(e) Activate all security force billets required during mobilization.

(f) Employ the Auxiliary Security Force (ASF) and MWD teams to protect mission essential assets.

(g) Respond to and recovery from incidents involving WMD.

(h) Incorporate AT awareness training information into the command's security education program and during

increased THREATCONs. This includes FP Level I briefings for personnel traveling to areas outside the United States and all personnel when the threat level rises above low within the U.S.

(i) Remain abreast of the capabilities and response of civilian and government agencies to respond to terrorist incidents (i.e., hospital capabilities, Emergency Medical Service (EMS) response, fire, Federal Bureau of Investigation (FBI), Federal Emergency Management Agency (FEMA), local and state civil defense organizations, local media, etc.).

(j) Inventory, account for and control arms, ammunition and explosives (AA&E).

(k) Review the process for new or modified construction. The Security Officer (or designated representative) shall review plans for new or modified construction during the design process and review phases to ensure that PS, loss prevention, AT and FP measures are adequately incorporated.

(3) Security surveys are an important part of the ongoing security review, assessment and management process. At a minimum, a survey should be conducted annually to identify changes, deficiencies, or additional requirements that affect the installation's overall FP posture. Completed surveys should be retained for 3 years per reference (e).

(4) The following assets require additional PS considerations, as outlined in Chapter 3 of reference (e), and will be addressed in PS plans where applicable. Waterfront security will be protected as a Level One restricted area and aviation assets will be protected as a Level Two restricted area. The following assets also require additional security considerations:

(a) Aircraft, ships, and other weapons systems/ platforms

(b) Communications systems

(c) Material/security (controlled inventory items)

(d) Bulk petroleum areas

(5) The plan must address the use of WMD, vulnerability of assets (if use of WMD occurs), planned countermeasures, and

the procedures for immediate notification to higher authority of use or potential use of WMD.

(6) The plan will be reviewed annually and updated to include any changes. Existing PS plans, meeting the requirements outlined above, are acceptable.

c. Waivers and Exceptions

(1) References (e) and (g) contain formats for requesting waivers/exceptions/extensions. The command PS/FP plan must include compensatory measures for all deficiencies. Regional and Installation Commanders will retain information copies of all waivers/exceptions until deficiencies are corrected.

(2) In addition to the waiver and exception authority outlined below, echelon III commands are delegated initial waiver approval authority for waivers under the cognizance of reference (g). Initial waiver authority, for waivers under the cognizance of reference (e), is not delegated.

Physical Security Issues
(OPNAVINST 5530.14C)

TYPE	DURATION	APPROVAL AUTHORITY
Initial Waiver	12 Months	CNET (OS4)
Waiver Extension	12-Month increments	CNO (N09N3) via CNET (OS45)
Exception Long Term	36 Months or longer	CNO (N09N3) via CNET (OS45)
Exception	Permanent	CNO (N09N3) via CNET (OS45)

Arms, Ammunition & Explosives Issues
(OPNAVINST 5530.13B)

TYPE	DURATION	APPROVAL AUTHORITY
Initial Waiver	12 Months	Echelon III
Waiver Extension	12-Month increments	CNO (N09N1) via NAVORDCEN (N72) CNET (OS414) and (OS45)
Exception	Permanent	CNO (N09N1) via NAVORDCEN (N72) CNET (OS414) and (OS45)

d. Loss Prevention. A vigorous loss prevention program is essential at every activity. Losses cost the government millions of dollars annually and can delay or prevent mission accomplishment. They must be minimized by the application of appropriate loss prevention measures. Effective loss reporting and maintenance of loss trend analysis are basic to determining the scope of the loss prevention program that must be developed. The DD Form 200 is used to report loss of government property. The DD Form 200 should be reviewed by the Regional/Installation Security Officer to determine if criminal activity has occurred and so loss prevention recommendations can be made.

4. Operations

a. Area Coordination. Successful physical security and force protection program planning and implementation require regional and whole installation cooperation to ensure economy of force and shared/efficient use of resources.

b. Threat Planning. An ongoing evaluation of threat types, threat assessments, and threat levels are essential to developing appropriate THREATCON responses. Based on available information, commands must determine the active short-, medium- and long-term threat. An annual threat assessment, through the servicing NAVCRIMINVSERV office, is required. Regional and Installation Commanders will develop creative and appropriate THREATCON measures that apply to assets and resources under their cognizance.

c. THREATCONS/Threat Type Definitions. THREATCONs and threat types definitions are addressed in references (c) and (e).

d. Antiterrorism

(1) AT measures must be reflected in PS programs, plans, exercises and operations.

(2) Commanders, commanding officers (COs), and officers in charge will ensure commands under their cognizance accomplish the following actions:

(a) Host commands must designate a commissioned Officer or GS-11 or above, in writing, as the Force Protection Officer (FPO). All other commands are required to designate an E-6 or above or GS-5 or above, in writing, as the Antiterrorist Training Officer (ATTO). FPOs and ATTOs must be graduates of the appropriate Level Two AT/FP training course prior to designation.

(b) Integrate antiterrorism measures into the overall FP program.

(c) Ensure procedures are in effect and disseminated for forwarding all information concerning locally emerging terrorist threats to CNET (in coordination with local NAVCRIMINVSERV representatives).

(d) Ensure a qualified ATTO or FPO conducts AT awareness training as part of required security education and for all personnel traveling on personal or official business outside the U.S., including Canada and Mexico.

(e) PS plans will cover AT measures and assigned tasking. The PS plan will outline actions required of each element in an organization relative to the applicable THREATCON in response to potential terrorist scenarios (bomb threats, hostage/captor situations, snipers, etc.). The plan will also provide for coordination with appropriate civilian and government agencies. Specifically, address capabilities of local civilian agencies to provide assistance and responsibilities to respond to terrorist incidents. These items will be defined formally in MOAs or MOUs.

(f) Conduct bomb evacuation drills in each building at least semiannually, more often if population turnover is more

frequent, and maintain documentation of drills. Personnel should practice evacuation procedures from different exits depending upon the location of the suspected bomb.

(g) Ensure billeting and primary gathering structures have interior and exterior audible bomb evacuation alarm systems installed that are unique from fire or other alarm systems. The system should be annunciated from within the building and a remote 24-hour monitored site. AT/FP construction standards will incorporate FP alarm systems as a DoD requirement and all new and refurbished structures will incorporate a bomb alarm system in the planning phases. Installation and regional commanders will program for funding to install alarm systems in existing buildings.

5. Training

a. Security Education and Training. Regional and Installation Commanders, through their appointed FP/Security Officers, will develop and establish FP/security education and training programs to ensure all assigned personnel, military and civilian, recognize and understand their responsibilities and role in preventing and reporting criminal and terrorist activity. All newly reporting personnel shall receive an initial command FP indoctrination briefing within 90 days of reporting for duty or employment. Refresher training should be conducted as needed. All completed training will be properly documented and retained for a period of 3 years. The content of the brief will be tailored to meet command security standards and inform personnel of their security responsibilities. Material contributed by the Command/Staff Judge Advocate, Medical, Disaster Preparedness, Safety, Public Affairs, NAVCRIMINVSERV and local law enforcement agencies should demonstrate the total security posture of the activity. As a minimum, the indoctrination briefing will include an overview of the following topics:

(1) Command FP instructions

(2) A general orientation on the need for everyone to be involved in keeping security measures in place

(3) How to recognize espionage and sabotage

(4) Personal protection measures

(5) Bomb threat actions

(6) Reporting of criminal and terrorist activity

(7) Reporting of security violations

b. Level I AT Awareness Training. Command ATTOs or FPOs will conduct AT/FP Level I training (individual AT awareness training) for all personnel (including family members of Permanent Change of Station (PCS) transferees) deploying or traveling outside of the U.S., including Canada and Mexico. This training will be conducted within the 6 months prior to deployment or travel and annually when the threat level rises above low in the U.S. Level I training consists of:

(1) Viewing the films "You may be the Target" and "Out of Harm's Way", receiving the Joint Staff Guide 5260 "Service Member's Personal Protection Guide: A Self-Help Handbook to Combating Terrorism" and the "Antiterrorism Individual Protective Measures" pocket card, listening to a 30-minute brief by a qualified FPO or ATTO which will include a specific area update for travelers going to known locations, and completion of documentation to include a Page 13 entry for military and a memo for the record for civilians.

(2) A certification of training will be annotated in the remarks section of travel/leave orders, on country clearance requests, and in the CO's overseas screening message for PCS orders.

c. Prospective CO/Executive Officer (XO) will receive Level III AT/FP training during their indoctrination training at CNET headquarters.

d. Naval Security Force (NSF) Education. NSF training will be conducted in accordance with the requirements of references (e), (h) and (k).

(1) All personnel performing physical security/law enforcement duties must successfully complete one of the following: Master-at-Arms (MA) or Law Enforcement course at Lackland Air Force Base (AFB), Phase I Basic Law Enforcement Training or the ASF course of instruction, as applicable, including small arms training and qualification. Annually or as required thereafter, NSF members shall complete the Phase II training course and weapons training contained in references (e) and (k).

(2) Specialized Training. Additional specialized training is necessary to fulfill safety requirements associated with working in the security field. Emergency vehicle operation, First Aid and cardiopulmonary resuscitation (CPR), traffic enforcement equipment standards, Small Arms Instructor Sustainment, and AA&E Screening requirements should be incorporated into security force training programs along with locally established training requirements.

(3) Regional and Installation Security Officers shall ensure effective security training programs are instituted at their activities. Training programs may be tailored to meet individual installation requirements. Comprehensive training plans should include:

(a) A region or installation-wide ASF training program.

(b) Development of training plans, schedules, written and practical tests, standard lesson topic guides and lesson topic guides that support special subjects unique to the region or installation.

(c) Establish and maintain individual training records.

(d) Maintain sufficient training facilities, supplies and equipment.

(e) Qualified instructors and assets to augment the Marine Cadre Mobile Training Team (MTT) training sessions.

(f) Periodic review of the entire training program to assess its overall quality.

(4) Regional Marine Cadre Training. The Regional Marine Cadre will provide the following training:

(a) Qualified instructors to conduct AT and weapons qualifications training to all members of the security force.

(b) Lesson topic guides to support the specific subjects contained in their course(s) of instruction.

(c) Support, guidance and assistance to the Installation Security Officer in administering and conducting the training program.

(5) Skills Evaluation. All security force personnel will be required to pass written and practical examinations to demonstrate their physical security knowledge/skills.

e. Security Officer Training Requirements

(1) Personnel assigned to the position of Security Officer, Security Department Head, or Security Director at a host command must be graduates of the Naval Physical Security and Law Enforcement Supervisors Course (NPSLESC) (S-830-0001) conducted by the NAVCRIMINVSERV, MTT, Atlantic (Quota Control: DSN 680-8925 or Comm (757) 462-8925) or attend the Navy Security Officers Course (A-7H-0004) held at Lackland AFB, San Antonio, Texas. Upon successful completion of the Lackland course, the student is certified as a Level II AT Training Officer and FPO (Quota control for Lackland is DSN 473-4824, Comm (210) 671-4824, e-mail: ken.woodworth@lackland.af.mil).

(2) Requests to waive these training requirements will be forwarded to CNET (OS45) for consideration. Equivalent prior training or experience will be considered on a case-by-case basis.

f. Exercises/Drills

(1) Reference (e) outlines minimum criteria for exercising security forces.

(2) Whenever possible, exercises should include all area law enforcement agencies to ensure total involvement of security forces.

(3) Copies of lessons learned from annual exercises and drills should be forwarded to CNET (OS45) within 30 days of completion of the exercise or drill.

6. Personnel

a. NSF

(1) The primary mission of the NSF is to provide security on board naval shore installations, vessels and aircraft. References (e), (h) and (l) provide guidance for assignment, employment, and organization of NSFs ashore.

(2) Minimum NSF training criteria is addressed in reference (e).

b. Auxiliary Security Force (ASF). All Navy installations (or regions) with a military population will form an ASF composed of personnel from the host and tenant activities, per reference (e).

(1) Composition. The number of ASF personnel assigned will be determined by the Regional/Installation Commander after assessing the threat and determining the number of posts which require manning.

(2) Training. Minimum ASF training criteria is addressed in reference (e).

7. Arming Security Force Personnel

a. Arming Security Force Personnel. The authority to arm personnel with firearms is delineated in SECNAVINST 5500.29B. Additionally, CNET installations shall ensure that personnel performing PS/law enforcement duties are qualified and armed with an appropriate weapon (i.e., 9mm pistol, M14/16 rifle, and/or 12-gauge shotgun). This includes:

(1) All law enforcement personnel, Civil Service Police/Guard series 083/085, MAs and personnel with Navy Enlisted Classification (NEC) 9545 when performing law enforcement/security duties.

(2) ASF personnel augmenting installation security forces.

(3) Seabees when assigned security duties.

b. Use of Force/Deadly Force. All personnel assigned to perform armed PS/law enforcement duties shall receive initial and periodic refresher training in the use of deadly force, per reference (e).

8. MWD Program. Regional/installation security forces use the MWD's unique capabilities to defend bases and their resources, and to help enforce military law and regulations. They supplement and enhance the security forces capabilities by allowing them to more effectively perform their mission. Regions/installations with MWD capabilities shall incorporate available certified resources into their daily operations. As a minimum, for

patrol-certified MWDs, this will include foot patrols in restricted areas (e.g., waterfront, piers, flightlines, fuels, etc.), non-restricted areas (e.g., housing, shopping areas, recreational areas, industrial areas, etc.), intruder detection and clearing, tracking, scouting, assignment to listening or observation posts, and assisting with administrative inspections.

9. WMD Planning

a. Each command will ensure there is a comprehensive WMD plan developed to meet MWD threats. Recent changes in the international availability of chemical and biological agents increase the possibility of a WMD attack or incident.

b. Background. The threat of WMD terrorism is different than the threat of Nuclear-Biological-Chemical ("NBC") used in combat. As events in Tokyo (1995 Sarin attack), New York City (1993 World Trade Center), and Oregon (1984 salmonella bacterium attack) indicate. The use of chemical and biologic agents in a terrorist attack are not only possible, but have been planned and executed. While these attacks have had varying success, it is undeniable that they have terrorized millions.

c. While the forward-deployed U.S. Navy is educated, trained and equipped to operate in a "NBC" environment, the rear areas and non-deployed forces are less so. To a terrorist looking to terrorize the U.S., an installation may make an inviting target. Many areas on the installation naturally tend to congregate unprotected people. Examples of these areas are the Navy Exchange, movie theaters, galleys and bachelor quarters. The Installation Commander should have a plan in place to mitigate the effects of WMD terrorism.

d. Some Critical Questions

(1) Who is the responsible person, staff or unit for WMD planning?

(2) What analysis products must be produced and for what purpose?

(3) What forces are assigned WMD detection, protection and decontamination responsibilities?

e. Considerations

(1) What changes will be made during increased THREATCON status to respond to the WMD threat?

(2) What forces will be required to accomplish these changes?

(3) What equipment, materials and time will be needed to make these changes?

f. WMD Threat Assessment

(1) What sources of information feed the threat assessment?

(2) What is the current threat?

(3) What terrorist groups have used WMD before?

(4) What type of agent has been used?

(5) What methods of dispersal have been attempted?

(6) Training levels of personnel in assessment?

g. Contamination Avoidance

(1) When was the last exercise that tested the contamination avoidance?

(2) Early warning?

(3) Sensor development and testing?

h. Protection

(1) What equipment is on hand?

(2) What protective gear is available to be issued?

(3) When was the last mission-oriented personal protection (MOPP) gear exercise?

(4) What were the results of the last MOPP exercise?

(5) What threat warning puts the installation in what posture (MOPP)?

i. Decontamination

(1) What decontamination gear is available for hasty/ deliberate decontamination?

(2) What are the threat agents?

(3) Where are the hospitals onbase/offbase?

(4) Where are the MOUs/MOAs that clearly lay out tasks and responsibilities?

10. Navy "Blue Dart" Terrorism Threat Warning Message

a. The Navy "Blue Dart" message is a means to disseminate an imminent terrorism threat warning to assets that are being targeted for terrorist attack. To qualify for a Navy "Blue Dart," the intelligence information must be credible, the terrorist threat must be directed against a specific Navy target, and the threat must contain a specific timeframe.

b. The Navy "Blue Dart" message will be disseminated by the Navy Antiterrorist Alert Center (NAVATAC) when intelligence indicates that a specific, imminent and credible terrorist attack will occur.

c. A Navy "Blue Dart" message requires acknowledgement by immediate message from all action addressees to DIRNAVCRIMINSERV WASHINGTON DC//NAVATAC/24//, info CNO WASHINGTON DC//N312//. Additionally, the affected unit should include their regular reporting chain of command in the info addee section. The Navy "Blue Dart" does not take the place of any existing reporting requirements. Any changes in the unit/installation's force protection status or threat condition should be noted in the initial response. Follow-up messages are encouraged if additional force protection measures are implemented. When a Navy "Blue Dart" message is received, commanders will:

(1) Review on-scene THREATCONS and liberty policies in the threatened area. Any modifications or defensive actions taken should be addressed by immediate message, through the chain of command, to DIRNAVCRIMINVSERV WASHINGTON DC //NAVATAC/24//, info CNO WASHINGTON DC//N312//.

(2) Protect threat warning information, to the maximum extent possible, consistent with the need to inform threatened units in a timely fashion.

(3) Dissemination of the threat information to potentially affected tenant commands is the responsibility of the Base/Installation Commander.

d. The primary means to communicate the threat warning will be via secure telephone where possible, unsecure if necessary. The base/installation or unit Command Duty Officer (CDO) will receive the information.

e. Exercise Navy "Blue Dart" messages will be issued in support of CNO Integrated VAs and specific major exercises on an ad hoc basis. Exercise Navy "Blue Dart" messages will assist the assessment teams and commanders in evaluating the information flow and force protection readiness of installations and units.

f. NAVATAC Navy "Blue Dart" messages will be addressed as follows:

(1) Action Addees. A "Blue Dart" will normally have only one action addee, the ship or unit that could be directly affected by a potential act of terrorism for which the NAVATAC has specific, imminent threat information. The only times a "Blue Dart" will have more than one action addee are:

(a) When multiple ships or units are affected.

(b) When the specific unit threatened is a tenant command of a larger region or installation. All units that are in a position to directly affect the security posture of the impacted unit will be action addees.

(2) Info Addees. Typical info addees will include the Fleet Commanders in Chief, the geographic Commanders in Chief, the regional intelligence centers, and the local NAVCRIMINVSERV office.

ANNEXES

CNET host command PS/FP plans have been added to this instruction as annexes but are not published with this instruction. Copies of the region/installation PS/FP plans are available in the CNET Security Program Manager's office (Room 2-72) (OS45).